EXHIBIT C-6
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 11 ('661 Patent)	U.S. 5,404,402 to Sprunk ("Sprunk")
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:7-13 – "The present invention relates generally to security apparatus for information processing systems and more particularly to the implementation of a secure microprocessor with reduced vulnerability to a security breach. The invention is particularly applicable to the secure transmission of scrambled television signals, although it is by no means limited to such use." 1:40-49 – "The ability of a pirate to observe such clock signals is critical in mounting a successful attack to the system security. However, such observation is nearly useless if the observation does not allow prediction of the clock signal in the future. It would therefore be advantageous to preclude the observation of a clock signal. It would be further advantageous to render the observation of a portion of a clock signal useless for predicting the future operation thereof." 2:40-49 – "The present invention also provides apparatus for clocking a cryptographic processor to reduce its vulnerability to attack. A stream of clock pulses is provided. Delay means are provided for delaying the pulses by a plurality of different selectable delays. One of the delays from the delay means is randomly selected for each clock pulse of the stream to provide an unpredictable stream of clock pulses. Means are provided for applying the unpredictable stream of clock pulses to a clock input of the cryptographic processor." 2:67-3:1 – "The cryptographic processor is clocked with the unpredictable clock signal to thwart efforts to observe a periodic behavior of the processor." 3:35-39 – "The present invention enhances the security of a secure microprocessor by rendering it extremely difficult, if not impossible, to observe a clock signal and predict the occurrence of subsequent clock pulses therefrom." Figure 1.
(a) an input interface for receiving a quantity to be cryptographically	4:9-13 – "The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to clock a conventional crypto processor 14 for the encryption or decryption of data entered via

Exhibit C-6 (Sprunk)

processed, said quantity being representative of at least a portion of a message;	terminal 16." Figure 1.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	4:9-13 – "The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to clock a conventional crypto processor 14 for the encryption or decryption of data entered via terminal 16."
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	4:9-13 – "The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to clock a conventional crypto processor 14 for the encryption or decryption of data entered via terminal 16." Figure 1.
(d) a noise production system for introducing noise into said measurement of said power consumption.	2:26-36 – "The random selection of a delay stage for each clock pulse can be accomplished using a plurality of linear feedback shift register generators of different lengths. The linear feedback shift register generators are responsive to prior clock pulses in the stream of pulses for outputting random control signals to select one of the delay stages for each successive clock pulse. Since the control signals allow the substantially random selection of a delay stage for each successive clock pulse, the occurrence of the successive clock pulses is substantially unpredictable." 2:67-3:1 – "The cryptographic processor is clocked with the unpredictable clock signal to thwart efforts to observe a periodic behavior of the processor." 3:67-4:13 – "A variable frequency source ('clock') 10 produces a clock signal with periodic clock pulses. Frequency source 10 can comprise an analog or digital circuit. For example, a tunable digital source (such as a ring oscillator), a tunable analog oscillator, or a plurality of selectable analog or digital fixed frequency oscillators can be used. Variable tuning or selection of the clock output frequency is effected using a substantially random 'modulation' circuit 12 that randomly varies each pulse of the clock signal to render the timing of successive pulses unpredictable. The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to

Exhibit C-6 (Sprunk)

	clock a conventional crypto processor 14 for the encryption or decryption of data entered via terminal 16."

Claim 29 ('661 Patent)	U.S. 5,404,402 to Sprunk
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:7-13 – "The present invention relates generally to security apparatus for information processing systems and more particularly to the implementation of a secure microprocessor with reduced vulnerability to a security breach. The invention is particularly applicable to the secure transmission of scrambled television signals, although it is by no means limited to such use." 1:40-49 – "The ability of a pirate to observe such clock signals is critical in mounting a successful attack to the system security. However, such observation is nearly useless if the observation does not allow prediction of the clock signal in the future. It would therefore be advantageous to preclude the observation of a clock signal. It would be further advantageous to render the observation of a portion of a clock signal useless for predicting the future operation thereof." 2:40-49 – "The present invention also provides apparatus for clocking a cryptographic processor to reduce its vulnerability to attack. A stream of clock pulses is provided. Delay means are provided for delaying the pulses by a plurality of different selectable delays. One of the delays from the delay means is randomly selected for each clock pulse of the stream to provide an unpredictable stream of clock pulses. Means are provided for applying the unpredictable stream of clock pulses to a clock input of the cryptographic processor." 2:67-3:1 – "The cryptographic processor is clocked with the unpredictable clock signal to thwart efforts to observe a periodic behavior of the processor." 3:35-39 – "The present invention enhances the security of a secure microprocessor by rendering it extremely difficult, if not impossible, to observe a clock signal and predict the occurrence of subsequent clock pulses therefrom." Figure 1.
(a) receiving a variable amount of power, said power consumption varying	4:9-13 – "The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to clock a conventional crypto processor 14 for the encryption or decryption of data entered via terminal 16."

Exhibit C-6 (Sprunk)

measurably during said performance of said operation;	Figure 1.
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	4:9-13 – "The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to clock a conventional crypto processor 14 for the encryption or decryption of data entered via terminal 16." Figure 1.
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	2:67-3:1 – "The cryptographic processor is clocked with the unpredictable clock signal to thwart efforts to observe a periodic behavior of the processor." 2:26-36 – "The random selection of a delay stage for each clock pulse can be accomplished using a plurality of linear feedback shift register generators of different lengths. The linear feedback shift register generators are responsive to prior clock pulses in the stream of pulses for outputting random control signals to select one of the delay stages for each successive clock pulse. Since the control signals allow the substantially random selection of a delay stage for each successive clock pulse, the occurrence of the successive clock pulses is substantially unpredictable." 2:63-3:8 – "A method is provided for clocking a cryptographic processor to reduce its vulnerability to attack. Clock pulses are randomly (i.e., completely or pseudorandomly) delayed in a clock stream to provide an unpredictable clock signal. The cryptographic processor is clocked with the unpredictable clock signal to thwart efforts to observe a periodic behavior of the processor. The pulses in the unpredictable clock signal are delayed at a varying rate within a range that does not extend beyond a minimum and maximum operating rate of the cryptographic processor. In a preferred embodiment, the range extends substantially from the minimum operating rate to the maximum operating rate of the cryptographic processor." 3:67-4:13 – "A variable frequency source ('clock') 10 produces a clock signal with periodic clock pulses. Frequency source 10 can comprise an analog or digital circuit. For example, a tunable digital source (such as a ring oscillator), a tunable analog oscillator, or a plurality of selectable analog or digital fixed frequency oscillators can be used. Variable tuning or selection of the clock output frequency is effected using a substantially random 'modulation' circuit 12 that

Exhibit C-6 (Sprunk)

	randomly varies each pulse of the clock signal to render the timing of successive pulses unpredictable. The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to clock a conventional crypto processor 14 for the encryption or decryption of data entered via terminal 16." 5:51-59 – "The output of multiplexer 26 is the unpredictable clock signal CLK which is used to clock a secure microprocessor, such as processor 14 illustrated in FIG. 1. The CLK clock signal is fed back within the ring oscillator for use in generating the next successive clock pulse. By selecting one of the eight possible delays on a substantially random basis for each successive clock pulse, the desired substantially random clock CLK is provided." Figure 1.
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:9-13 – "The unpredictable pulse stream 'CLK' is output from the variable frequency source 10 and used to clock a conventional crypto processor 14 for the encryption or decryption of data entered via terminal 16." Figure 1.